ABSTRACT OF THE DISCLOSURE

Technique for protecting a communications network, such a computer network, from attack such as self-propagating code violations of security policies, in which the network is divided into "compartments" that are separated by access control devices such as firewalls. The access control devices are then used to stop the spread of self-propagating attack code, the "zero-day" worms, for example. However, the access control devices are configured such that upon activation legitimate in-use network services will not be jeopardized.